IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In Re Application Of:	§	**Atty. Docket No. RPS920030206US2**
RYAN CHARLES CATHERMAN	§	**Examiner: TURCHEN, JAMES R.**
Serial No.: 10/749,261	§	**Art Unit: 2139**
Filed: DECEMBER 31, 2003	§	**Conf. no.: 8466**
For: METHOD FOR SECURELY CREATING AN ENDORSEMENT CERTIFICATE UTILIZING SIGNING KEY PAIRS	§	

APPEAL BRIEF UNDER 37 C.F.R. 41.37

Mail Stop Appeal Briefs - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

This Brief is submitted in support of the Appeal of the Examiner's final rejection of Claims 1-6, 8, 10-15, 17-22 and 24 in the above-identified application. A Notice of Appeal was filed in this case and received in the Patent Office on February 17, 2009. A one-month extension of time is required to submit this Appeal Brief and is hereby requested. Please charge the fee of $130.00 for the extension of time to **DILLON & YUDELL LLP Deposit Account No. 50-3083**. Please charge the fee of $510.00 due under 37 C.F.R. §1.17(c) for filing the brief, as well as any additional required fees, to **IBM's Deposit Account No. 09-0447**.

05/19/2009 HMARZI1 00000018 090447 10749261
01 FC:1402 540.00 DA

05/19/2009 HMARZI1 00000018 090447 10749261
02 FC:1251 130.00 DA

REAL PARTY IN INTEREST

The real party in interest in the present Application is International Business Machines Corporation, the Assignee of the present application as evidenced by the Assignment set forth at reel 014801, frame 0608.

RELATED APPEALS AND INTERFERENCES

An appeal of the final action in patent application Ser. No.: 10/750,594, which appeal was filed on May 18, 2009, may affect or be directly affected by or have a bearing on the Board's decision in the present appeal. There are no other appeals or interferences known to Appellants, the Appellants' legal representative, or assignee, which directly affect or would be directly affected by or have a bearing on the Board's decision in the pending appeal.

STATUS OF CLAIMS

Claims 1-6, 8, 10-15, 17-22 and 24 stand finally rejected by the Examiner as noted in the Final Office Action dated September 17, 2008. The rejection of Claims 1-6, 8, 10-15, 17-22 and 24 is appealed.

STATUS OF AMENDMENTS

No amendment was made subsequent to the Final Action from which this appeal is taken.

SUMMARY OF THE CLAIMED SUBJECT MATTER

As recited by Appellants' example method Claim 1 (and corresponding system Claim 17), Appellants' invention provides a method (FIGs. 4 and 5) for securely creating an endorsement certificate for a device in an insecure environment. The method comprises: generating for a valid device (FIG. 2) an endorsement key pair that includes a private key and a public key, wherein said private key is not public readable (¶¶ 0036, 0039; FIG. 4, 403); creating a non-public, signing key pair that is injected into a plurality of valid devices, wherein the signing key pair is a first signing key pair that is provided to a first set of said plurality of valid devices and a second set of said plurality of valid devices are provided a second signing key pair, based on a pre-defined method for determining when to switch from utilizing said first signing key pair to utilizing said second signing key pair, said pre-defined method selected from among:

expiration of a preset amount of device manufacturing time; and manufacture of a preset number of devices from the plurality of valid devices (*see* ¶ 0040, 0041). The method further comprises: verifying at a credential server that an endorsement key of a requesting device is a valid endorsement key generated during manufacture of said valid device by confirming a signature of said endorsement key is a public signing key of said signing key pair, wherein said credential server includes secure identification data of said non-public, signing key pair (*see* ¶ 0045, 0046; FIG. 4, 415, 416); and inserting an endorsement certificate into said device to indicate that said device is an approved device by an OEM (original equipment manufacturer) of the device only when said endorsement key is confirmed having been generated from within a valid device (*see* ¶ 0046, 0047; FIG. 4, 417, 419, 421; *see* also FIG. 5, ¶¶ 0049-0051). The signing key pair is a single-use parameter (¶ 0044), and the method further comprises immediately destroying said signing key pair within said device following a creation of said endorsement key (EK) (¶ 0044).

Appellants' Claim 2 (and corresponding system Claim 18) provides: providing a signing key certificate for said signing key pair (¶ 0042), said signing key certificate including a public signing key of said signing key pair (¶ *see* 0045); and forwarding said signing key certificate via a secure communication medium to said credential server (*see* ¶ 0045; FIG. 4, 405).

Appellants' Claim 3 further provides: signing said public key of the endorsement key pair with a public signing key of said signing key pair when creating the endorsement key (EK) (¶ 0047; FIG. 4, 411); and forwarding a resulting signed EK to said credential server to initiate a credential process (*see* ¶ 0048; FIG. 4, 415).

Appellants' Claim 4 (and corresponding system Claim 20) provides: receiving said signed EK at said credential server (¶ 0049; FIG. 4, 416); comparing the public signing key within the signing key certificate with a signature from the signed EK (*see* ¶ 0049; FIG. 4, 417); and when the public signing key matches the signature, confirming said EK as originating from a valid device (¶ 0049, 0050; FIG. 4, 419).

Appellants' Claim 5 (and corresponding system Claim 21) further provides: initially storing the credential in a database of said credential server (*see* ¶ 0052; FIG. 5, 503);

monitoring for a request from a customer to provide said certificate to said device (¶ 0053; FIG. 5, 502); and following a receipt of said customer request, transmitting said certificate to said device to be inserted within the device (*see* ¶ 0053; FIG. 5, 505, 507).

Appellants' Claim 6 (and corresponding system Claim 22) provides: wherein said endorsement certificate is once-writeable public-readable and is utilized for signing said public key during communication from and to said device (¶ 0049).

Appellants' Claim 8 (and corresponding system Claim 24) further provides: wherein said credential server is remotely located from a vendor manufacturing said device and said method comprises transmitting said signing key pair from said device to said credential server via a secure communication medium (*see* ¶ 0054).

Appellants' Claim 10 provides: wherein said device is a trusted platform module (TPM) (*see* ¶ 0034, 0036; FIG. 1, 150; FIG. 2).

Appellants' Claim 11 further provides: a TPM device manufactured and authenticated according to the steps of Claim 1 (FIGs. 4 and 5).

Appellants' Claim 13 (incorporating the features of base Claim 12) further provides a data processing system comprising: a processor 150; a trusted platform module (TPM) chip 150; a bus for interconnecting said processor and said TPM chip; a network interface with communication means for connecting said TPM to a secure credential server 107; and means, whereby said TPM 150 is able to verify an endorsement key (EK) pair of said TPM as being a valid pair generated during manufacture of said TPM by utilizing a signing key pair injected by a TPM vendor into the TPM during manufacture (103) of the TPM, wherein said signing key pair is a single-use parameter (¶ 0044), said data processing system further comprising means for immediately destroying said parameter within said device following a creation of the EK (¶ 0044). The signing key pair has an associated signing key certificate that is sent to the secure credential server during manufacture of the TPM (¶ 0045). The means for verifying an endorsement key pair further comprises: means for signing a public value of said endorsement

key pair with a public signing key of said signing key pair to generate a signed (EK) (¶¶ 0045-0046); and means for forwarding said signed EK to said credential server, wherein said credential server returns an endorsement certificate only when the signed EK was generated within the TPM as confirmed by a comparison of the signed EK's public signing key with a public signing key of the signing key certificate (¶¶ 0045-0047; FIG. 4; *see* also FIG. 5, ¶¶ 0049-0051).

Appellants' Claim 14 provides a data processing system 104 utilized for issuing endorsement certificates. The data processing system 104 comprises: a processor; a memory couple to said processor via an interconnect; a security mechanism for ensuring optimum security of processes within said data processing system; input/output mechanism for receiving a signing key certificate from a TPM vendor for utilization during a credential process for a specific group of manufactured TPM devices; and secure communication means for receiving an endorsement key (EK) requesting issuance of an endorsement certificate, wherein said EK comprises a public endorsement key signed by a public signing key. Further, the data processing system comprises program means for: determining, by utilizing said public signing key and said signing key certificate, when said EK is an EK of an endorsement key pair that was generated within one of said manufactured TPM devices; recording when a request for EK certificate fails (FIG. 4, 423; ¶ 0048; *see* also FIG. 5, ¶¶ 0049-0051); tracking each failed request to identify TPM vendors with greater than a pre-established number of failures (*see* ¶ 0051; FIG. 4, 423); and messaging said TPM vendors to update their security procedures (¶ 0051; FIG. 4).

Appellants' Claim 15 further provides: means for generating a certificate only when said public signing key matches a public signing key within said signing key certificate (*see* ¶ 0050; FIG. 4).

Appellants' Claim 19 further provides: means for combining said public key of the endorsement key pair with a public signing key of said signing key pair when creating the endorsement key (EK) (¶ 0047; FIG. 4); and means for forwarding a resulting signed EK to said credential server to initiate a credential process (*see* ¶ 0047; FIG. 4).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. The Examiner's rejection of Claims 1-6, 8, 10-22 and 24 under 35 U.S.C. §103(a) as being unpatentable over *Challener* (U.S. Patent Publication No. 2002/0169717) in view of *Smith* (U.S. Patent No. 6,233,685) and further in view of *Wood* (U.S. Patent Publication No. 2006/0072747) is to be reviewed on Appeal.

B. The Examiner's rejection of Claims 14 and 15 under 35 U.S.C. §103(a) as being unpatentable over *Challener* in view of *Felt* (U.S. Patent Publication No. 2002/0138735) is to be reviewed on Appeal.

ARGUMENT

A. The rejection of Claims 1-6, 8, 10-22 and 24 as being unpatentable over *Challener* in view of *Smith* and further in view of *Wood* is not well founded and should be reversed.

A. 1 General requirements for a claim rejection under 35 U.S.C. § 103

According to 35 U.S.C. §103(a):

> A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Examiner improperly rejects Claims 1-6, 8, 17-22, and 24 as being unpatentable over *Challener* in view of *Smith* and further in view of *Wood* under 35 USC §103. The combination of references does not render Appellants' claimed invention unpatentable because that combination does not render obvious, to one skilled in the art at the time of Appellants' invention, several of the features recited by Appellants' claims. For example, the combination fails to render obvious the following features (among others) of Appellants' independent Claims 1 and 17:

> (a) creating a non-public, signing key pair that is injected into a plurality of valid devices, wherein the signing key pair is a first signing key pair that is provided to a first set of said plurality of valid devices and a second set of said plurality of valid devices are provided a second signing key pair, based on a pre-defined method for determining when to switch from

utilizing said first signing key pair to utilizing said second signing key pair, said pre-defined method selected from among: expiration of a preset amount of device manufacturing time; and manufacture of a preset number of devices from the plurality of valid devices.

(b) wherein said signing key pair is a single-use parameter, said method further comprising immediately destroying said signing key pair within said device following a creation of said endorsement key (EK).

To establish a prima facie case of obviousness, one of the three basic criteria requires the prior art reference (or references when combined) teach or suggest all the claim limitations. *Challener* in view of *Smith*, fail to teach all the claim limitations. On page 5 of the Office Action, in explaining the motivation to combine *Challener* in view of *Smith*, the Examiner states "[i]t would have been obvious to one of ordinary skill in the art at the time if the invention to combine the method of *Challener* for generating an endorsement key, creating a signing key, and inserting an endorsement certificate with the method of *Smith* et al. for verifying that a key is in fact a key from the device in order to certify the device".

Neither *Challener* nor *Smith* suggest the generation of a public and private key as taught within the Appellants' claimed invention, nor could anyone of ordinary skill in the art modify *Challener* or *Smith* to render Appellants' claimed invention obvious. With respect to the references, the Examiner admits "*Challener* does not disclose wherein the signing key pair is a first signing key pair that is provided to a first set of said plurality of valid devices and a second set of said plurality of valid devices..." (Office Action, page 4). However, the Examiner improperly ignores the importance of Appellants' novel claim feature for creating the non-public, signing key pair as presented within Claims 1 and 17. As recited by these claims, the creation of the non-public, signing key pair is "based on a pre-defined method for determining when to switch from utilizing said first signing key pair to utilizing said second signing key pair". The Examiner simply assumes "[i]t would have been obvious to one of ordinary skill in the art...to modify the key pair to change from a single device to a plurality of devices" (Office Action, page 5 of). The Examiner negates a primary feature of Appellants' independent claim in arriving at the flawed obviousness conclusion.

Further, the Examiner correctly indicates "*Challener* and *Smith* do not teach wherein said signing key pair is a single use parameter, said method further comprising immediately destroying said signing key pair within said device following a creation of said endorsement key" (Office Action, page 5-6). However, when comparing Appellants' claim elements to *Wood et al.* the Examiner draws an obviousness conclusion, but utilizes only a small portion of Appellants' claim element. The Examiner states "*Wood* et al. discloses using a temporary key pair...after which the key is no longer used" (Office Action, page 6). The Examiner ignores Appellants' claim feature which more completely states "said signing key pair is a single-use parameter, said method further comprising immediately destroying said signing key pair within said device **following a creation of said endorsement key**" (bold added for emphasis). Neither *Challener*, *Smith*, nor *Wood* teach or suggest "said signing key pair is a single-use parameter, said method further comprising immediately destroying said signing key pair within said device following a creation of said endorsement key" as presented by Appellants' independent claims.

The Examiner has ignored vital features of Appellants' claimed invention to create an obviousness argument. The Examiner has not properly evaluated specific features of Appellants' Claims 1 and 17, which features demonstrate the novelty of Appellants' claimed invention, and which features are not taught or suggested by none of *Challener*, *Smith*, nor *Wood*. Accordingly, the Examiner has failed to meet at least one criterion required to establish a prima facie case of obviousness, which criterion requires that the prior art references must teach or suggest all the claim limitations.

Moreover, Claims 2-6, 8, 10-11 depend on independent Claim 1, and Claims 18-22, 24 depend on independent Claim 17. Appellants have shown by the above arguments that both Claims 1 and 17 are allowable over the combination of references. By the dependence of Claims 2-6, 8, 10-11 on an allowable base Claim 1 and the dependence of Claims 18-22, 24 on an allowable base Claim 17, the present dependent claims are therefore also allowable. The rejection of Appellant's Claims 2-6, 8, 10-11 and Claims 18-22, 24 is thus not well founded and should be reversed.

From the above discussion/arguments and the reasons provided therein, it is clear that the combination of references does not render obvious key features of Appellants' claimed invention. One skilled in the art would not find Appellants' claimed invention unpatentable over the combination of references. The rejection of Claims 1-6, 8, 10-11, 17-22, and 24 for the above reasons, is not well founded and should be reversed.

B. The rejection of Claims 14 and 15 under 35 U.S.C. §103(a) as being unpatentable over *Challener* in view of *Felt* is not well founded and should be reversed.

First, Appellants assert that the above combination is improper. Second, even if found to be proper, the combination would still not render Appellants' claimed invention unpatentable because the combination does not suggest the subject matter recited by Appellants' claims to one skilled in the art at the time of Appellants' invention.

B.1. No motivation to combine

First, with respect to the above references, there is no motivation to combine *Challener* with *Felt* in the manner done by the Examiner. The proper rationales for arriving at a conclusion of obviousness, as indicated by the U.S. Supreme Court in the case of *KSR International Co. v. Teleflex, Inc. et al.*, 127 S. Ct. 1727 (2007), hereinafter *KSR*, include the following tests for determining a motivation to combine elements from the prior art:

> A. Combining prior art elements according to known elements to yield predictable results;
> B. Simple substitution of one known element for another to obtain predictable results;
> C. Use of a known technique to improve similar devices in the same way;
> D. Applying a known technique to a known device ready for improvement to yield predictable results;
> E. "Obvious to try" – choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success;
> F. Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrived at the claimed invention.

(all emphasis added.)

There is no teaching within *Challener* or *Felt* that would motivate one skilled in the art at the time of Appellants' invention to combine the features of the two references. Further, there is

no motivation or support for the proposed combination of *Challener* or *Felt* in either reference or under any of the above *KSR* rationales for making a proper combination under §103. Therefore, the combination is improper.

On page 9 of the Office Action, in explaining the motivation to combine *Challener* or *Felt*, Examiner states: "[i]t would have been obvious to one of ordinary skill in the art ... to modify the system ... with the system of auditing and reporting ... in order to form a recorded history making it easier to track down intermittent problems." It is therefore clear that, under *KSR*, Examiner relies on the "teaching, suggestion, and motivation" test with the rationale of "obvious to one of ordinary skill in the art" to support the combination and determine obviousness.

Appellants' respectfully disagree with Examiner's conclusions under this rationale because the two references do not themselves suggest, teach or motivate one skilled in the art to make the combination. The Examiner admits on page 9 of the Office Action that "*Challener* does not disclose an event auditing and reporting system". A close read of *Felt* reveals that *Felt* does not teach or suggest: recording when a request for EK certificate fails; tracking each failed request to identify TPM vendors with greater than a pre-established number of failures; and messaging said TPM vendors to update their security procedures, nor any other feature provided within Appellants' example Claim 14. Any possible connection between the teachings of *Challener* with the teachings of *Felt* would be so tangential in nature that one skilled in the relevant art would not have been inclined to combine the two references. There is, therefore, no support within the references themselves for combining the references, and one skilled in the art would not have been motivated to combine the references. Thus, Appellants again assert that this combination is improper, and Claim 14 is allowable.

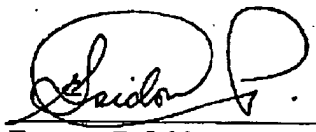
Further, Claim 15 depends on independent Claim 14, which Appellants have shown by the above arguments to be allowable over the combination of references. By the dependence of Claim 15 on an allowable base Claim 14, the present dependent claim is therefore also allowable. The rejection of Appellant's Claim 14 is thus not well founded and should be reversed.

The above deficiencies in the teachings/suggestions of *Challener* and *Felt* indicate that the combination of these references does not teach or suggest several features recited within Appellants' claims. Thus, one skilled in the art would not find Appellants' invention unpatentable over the combination of references. Appellants' Claim 14-15 are therefore allowable over the combination, and Examiner's rejection of these claims is not well founded and should be reversed.

CONCLUSION

Appellants have pointed out with specificity the manifest error in the Examiner's rejections and the claim language which renders the invention patentable over the primary reference and the various combinations of references. Appellants, therefore, respectfully request that this case be remanded to the Examiner with instructions to issue a Notice of Allowance for all pending claims.

Respectfully submitted,



Eustace P. Isidore
Reg. No. 56,104
DILLON & YUDELL LLP
8911 N. Capital of Texas Highway
Suite 2110
Austin, Texas 78759
512-343-6116

ATTORNEY FOR APPELLANTS

APPENDIX

1. A method for securely creating an endorsement certificate for a device in an insecure environment, said method comprising:

generating for a valid device an endorsement key pair that includes a private key and a public key, wherein said private key is not public readable;

creating a non-public, signing key pair that is injected into a plurality of valid devices, wherein the signing key pair is a first signing key pair that is provided to a first set of said plurality of valid devices and a second set of said plurality of valid devices are provided a second signing key pair, based on a pre-defined method for determining when to switch from utilizing said first signing key pair to utilizing said second signing key pair, said pre-defined method selected from among:

expiration of a preset amount of device manufacturing time; and

manufacture of a preset number of devices from the plurality of valid devices;

verifying at a credential server that an endorsement key of a requesting device is a valid endorsement key generated during manufacture of said valid device by confirming a signature of said endorsement key is a public signing key of said signing key pair, wherein said credential server includes secure identification data of said non-public, signing key pair; and

inserting an endorsement certificate into said device to indicate that said device is an approved device by an OEM (original equipment manufacturer) of the device only when said endorsement key is confirmed having been generated from within a valid device;

wherein said signing key pair is a single-use parameter, said method further comprising immediately destroying said signing key pair within said device following a creation of said endorsement key (EK).

2. The method of Claim 1, further comprising:

providing a signing key certificate for said signing key pair, said signing key certificate including a public signing key of said signing key pair; and

forwarding said signing key certificate via a secure communication medium to said credential server.

3. The method of Claim 1, further comprising:

signing said public key of the endorsement key pair with a public signing key of said signing key pair when creating the endorsement key (EK); and

forwarding a resulting signed EK to said credential server to initiate a credential process.

4. The method of Claim 3, further comprising:

receiving said signed EK at said credential server;

comparing the public signing key within the signing key certificate with a signature from the signed EK; and

when the public signing key matches the signature, confirming said EK as originating from a valid device.

5. The method of Claim 1, wherein following said verifying step said method further comprises:

initially storing the credential in a database of said credential server;

monitoring for a request from a customer to provide said certificate to said device; and

following a receipt of said customer request, transmitting said certificate to said device to be inserted within the device.

6. The method of Claim 1, wherein said endorsement certificate is once-writeable public-readable and is utilized for signing said public key during communication from and to said device.

7. (canceled)

8. The method of Claim 1, wherein said credential server is remotely located from a vendor manufacturing said device and said method comprises transmitting said signing key pair from said device to said credential server via a secure communication medium.

9. (canceled)

10. The method of Claim 1, wherein said device is a trusted platform module (TPM).

11. A TPM device manufactured and authenticated according to the steps of Claim 1.

12. A data processing system comprising:

a processor;

a trusted platform module (TPM) chip;

a bus for interconnecting said processor and said TPM chip;

a network interface with communication means for connecting said TPM to a secure credential server; and

means, whereby said TPM is able to verify an endorsement key (EK) pair of said TPM as being a valid pair generated during manufacture of said TPM by utilizing a signing key pair injected by a TPM vendor into the TPM during manufacture of the TPM, wherein said signing key pair is a single-use parameter, said data processing system further comprising means for immediately destroying said parameter within said device following a creation of the EK.

13. The data processing system of Claim 12, wherein said signing key pair has an associated signing key certificate that is sent to the secure credential server during manufacture of the TPM and said means for verifying an endorsement key pair further comprises:

means for signing a public value of said endorsement key pair with a public signing key of said signing key pair to generate a signed (EK); and

means for forwarding said signed EK to said credential server, wherein said credential server returns an endorsement certificate only when the signed EK was generated within the TPM as confirmed by a comparison of the signed EK's public signing key with a public signing key of the signing key certificate.

14. A data processing system utilized for issuing endorsement certificates, comprising:

a processor;

a memory couple to said processor via an interconnect;

a security mechanism for ensuring optimum security of processes within said data

processing system;

input/output mechanism for receiving a signing key certificate from a TPM vendor for utilization during a credential process for a specific group of manufactured TPM devices; and

secure communication means for receiving an endorsement key (EK) requesting issuance of an endorsement certificate, wherein said EK comprises a public endorsement key signed by a public signing key; and

program means for:

determining, by utilizing said public signing key and said signing key certificate, when said EK is an EK of an endorsement key pair that was generated within one of said manufactured TPM devices;

recording when a request for EK certificate fails;

tracking each failed request to identify TPM vendors with greater than a pre-established number of failures; and

messaging said TPM vendors to update their security procedures.

15. The data processing system of Claim 14, further comprising means for generating a certificate only when said public signing key matches a public signing key within said signing key certificate.

16. (canceled)

17. A system for securely creating an endorsement certificate for a device in an insecure environment, said system comprising:

means for generating for a valid device an endorsement key pair that includes a private key and a public key, wherein said private key is not public readable;

means for creating a non-public, secure value that is provided to both a plurality of valid devices and a credential server, wherein the signing key pair is a first signing key pair that is provided to a first set of said plurality of valid devices and a second set of said plurality of valid devices are provided a second signing key pair, based on a pre-defined system for determining when to switch from utilizing said first signing key pair to utilizing said second signing key pair, said pre-defined system selected from among:

expiration of a preset amount of device manufacturing time; and

manufacture of a preset number of devices from the plurality of valid devices;

means for verifying at a credential server that an endorsement key (EK) of a requesting device is a valid endorsement key generated during manufacture of said valid device by confirming a signature of said endorsement key is a public signing key of said signing key pair, wherein said credential server includes secure identification data of said non-public, signing key pair; and

means for inserting an endorsement certificate into said device to indicate that said device is an approved device by an OEM (original equipment manufacturer) of the device only when said endorsement key is confirmed having been generated from within a valid device;

wherein said signing key pair is a single-use parameter, said system further comprising means for immediately destroying said parameter within said device following a creation of said EK.

18. The system of Claim 17, further comprising:

means for providing a signing key certificate for said signing key pair, said signing key certificate including a public signing key of said signing key pair; and

means for forwarding said signing key certificate via a secure communication medium to said credential server.

19. The system of Claim 18, further comprising:

means for combining said public key of the endorsement key pair with a public signing key of said signing key pair when creating the endorsement key (EK); and

means for forwarding a resulting signed EK to said credential server to initiate a credential process.

20. The system of Claim 19, further comprising:

means for receiving said EK from said credential server;

means for comparing the copy of the public signing key within the signing key certificate with a signature from the signed EK; and

means, when the public signing keys match, for confirming said EK as originating from a

valid device.

21. The system of Claim 17, wherein following said verifying said system further comprises:

means for initially storing the credential in a database of said credential server;

means for monitoring for a request from a customer to provide said certificate to said device; and

means for following a receipt of said customer request, transmitting said certificate to said device to be inserted within the device.

22. The system of Claim 17, wherein said endorsement certificate is once-writeable public-readable and is utilized for signing said public key during communication from and to said device.

23. (canceled)

24. The system of Claim 17, wherein said credential server is remotely located from a vendor manufacturing said device and said system comprises means for transmitting said signing key certificate from said device to said credential server via a secure communication medium.

25. (canceled)

EVIDENCE APPENDIX

Other than the Office Action(s) and reply(ies) already of record, no additional evidence has been entered by Appellants or the Examiner in the above-identified application which is relevant to this appeal.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings as described by 37 C.F.R. §41.37(c)(1)(x) known to Appellants, Appellants' legal representative, or assignee.